Analisi Malware

Traccia:
La figura nella slide successiva mostra un estratto del codice di un malware. Identificate:
1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

Figura 1:

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

1. Prendendo in considerazione le due chiamate della funzione: push WH_Mouse e call SetWindowHook(), possiamo dedurre che il malware sia un keylogger che identifica dove va a cliccare il mouse.
2. Call SetWindowHook() = gli hook di sistema in genere servono per intercettare quello che avviene sul sistema operativo o nelle finestre. In questo caso in push precedente ci dice che sta intercettando i movimenti e click del mouse.
   Call CopyFile() = serve per salvare il malware in una determinata porzione di memoria.
3. La persistenza viene acquisita dal malware con la call CopyFile(); cioè il malware copia se stesso nel path indicato: <<path to start_folder_system>>

4. push eax
   push abx
   push ecx
   Si crea un nuovo stack

push WH_Mouse ; hook to Mouse
call SetWindowsHook()
prepara l'argomento per la chiamata della funzione, cioè il puntatore del mouse, per poi chiamare la funzione, cioè installare un hook che intercetta i movimenti e click del mouse.

XOR ECX,ECX imposta il registro ecx a zero, cioè lo ripulisce per poi salvarci il malware

mov ecx, [EDI] EDI = «path to startup_folder_system»
mov edx, [ESI] ESI = path_to_Malware
push ecx ; destination folder
push edx ; file to be copied
Questo blocco sposta il malware nel path dove verrà poi copiato e salvato, per poi mettere il contenuto nella cartella di destinazione, push edx mette il contenuto nel registro edx (cioè mette il malware nel registro edx dello stack).

call CopyFile() ottiene la persistenza. Il malware viene copiato nella cartella di destinazione indicata precedentemente, in questo modo il malware verrà eseguito ad ogni avvio in quanto la cartella indicata e quella startup_folder_system.